UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,306	10/14/2005	Yuliang Zheng	56697-326363	1967

44231 7590 02/20/2008
KILPATRICK STOCKTON LLP - 46872
J. STEVEN GARDNER
1001 WEST FOURTH STREET
WINSTON-SALEM, NC 27101

EXAMINER	
HUSSAIN, IMAD	

ART UNIT	PAPER NUMBER
2151	

MAIL DATE	DELIVERY MODE
02/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/553,306	**Applicant(s)** ZHENG ET AL.
	Examiner IMAD HUSSAIN	**Art Unit** 2151

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____is/ are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 09 January 2008 has been received and made of record.

2. Amended claims 1-17 are pending in application 10/553306.

3. Amendment to claim(s) 4 in response to objection has been considered. The amendment to the claims obviates previously raised rejection. As such this objection is hereby withdrawn.

Claim Rejections - 35 USC § 112

4. Claim 4 rejected under 35 U.S.C. 112, first Paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Amended claim 4 recites the limitation that the threshold value is inversely proportional to the service value. In the original disclosure and claims as originally filed, it is stated that the threshold value is inversely proportional to the **node** value [Claim 3 and Glossary: Threshold].

Claim Rejections - 35 USC § 102

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1, 2 and 5-17 are rejected under 35 U.S.C. 102(e) as being anticipated by John B. Beavers (US PGPub 2003/0221123 A1, hereafter Beavers).

Regarding claim 1, Beavers teaches a network security system, comprising:

a static policy data store [*set of rules*, claim 1 and *rule engine,* Figure 5 (27)] having a static policy data attribute [*customer-specific enterprise rules*, Paragraph 0075];

a dynamic policy data store [*decision table*, claim 1 and Figure 5 (31); *dynamic threat table*, Paragraph 0054; *dynamic tracking table*, Paragraph 0098] for tracking a threat level associated with a connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114], the dynamic policy store having a dynamic policy data attribute [*assets… and… alerts/categories… automatically recorded… for later pattern recognition and possible automated declaration of incidents*, Paragraph 0054];

an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with the static policy data store [*Rule Engine*, Figure 5 (27)] and the dynamic policy data store [*Decision Tables*, Figure 5 (31)] and operable to perform a risk-aware analysis [*matching* and *declaring an incident*, claim 1] of the connection to determine the threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection based at least in part on the static policy data attribute [*static enterprise data... such as lists of IP addresses that are associated with known attackers,* Paragraph 0077].

Regarding claim 2, Beavers teaches that the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value [*a threshold value from a user-editable table*, claim 5], a node value, a service value, and an action value.

Regarding claim 5, Beavers teaches that the dynamic policy data store comprises a threat level table [*table with threat characterizations*, claim 5].

Regarding claim 6, Beavers teaches that the system is further operable to generate a response to the connection [*an action as a mitigating response can be taken*, Paragraph 0039].

Regarding claim 7, Beavers teaches that the response comprises at least one of blocking the source of the connection from connecting to an intended destination [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised,* Paragraph 0039], altering the intended destination of the connection [after an alert, *the information is trashed or diverted at line 25*, Paragraph 0033], or auditing the connection [Paragraph 0003].

Regarding claim 8, Beavers teaches that the AEF is further operable to generate a countermeasure [*an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised,* Paragraph 0039].

Regarding claim 9, Beavers teaches that the countermeasure comprises a passive countermeasure [Beavers: *an action as a mitigating response can be taken. An example would be to shut down a web server that is suspected of being compromised,* Paragraph 0039].

Regarding claim 10, Beavers teaches that the system comprises a router, a gateway, a hardware appliance [*firewall, IDS, router,* etc., Paragraphs 0105-0114], or a web server [claim 15].

Regarding claim 11, Beavers teaches that the system further comprises a firewall [Paragraph 0109] in communication with the AEF [*alert processing system*].

Regarding claim 12, Beavers teaches that the system further comprises an intrusion detection system [*IDS,* Paragraph 0113] in communication with the AEF [*alert processing system*].

Regarding claim 13, Beavers teaches a method comprising:

receiving a static policy data attribute [*customer-specific enterprise rules*, Paragraph 0075] from a static policy data store [*set of rules,* claim 1; Fig 5 (27)];

receiving a connection request directed to a node [Paragraphs 0002-0003];

determining a threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114] based at least in part on the static policy data attribute [*set of rules,* claim 1 including *customer-specific enterprise rules*, Paragraph 0075] ; and

storing the threat level associated with the connection request as a dynamic policy data attribute [*assets... and... alerts/categories... automatically recorded... for later pattern recognition and possible automated declaration of incidents*, Paragraph 0054] in a dynamic policy data store [*decision table,* claim 1].

Regarding claim 14, the claim comprises the limitations of claims 13 and 6 and is rejected by the same rationale.

Regarding claim 15, the claim comprises the limitations of claims 14 and 7 and is rejected by the same rationale.

Regarding claim 16, Beavers teaches updating the dynamic policy data attribute in the dynamic policy data store based on a result of the determining [*incident tracking rules* *can be automatically updated based on one or more further alert indications*, Paragraph 0015].

Regarding claim 17, Beavers teaches increasing a threat level if the connection request is determined to be anomalous [*If the non-condition alert passes the threshold, this information can be added to existing incident tickets, and the incident ticket tracking rules can be updated with this information*, Paragraph 0097; the rules referencing *the table with the time, the status, the threat level, and an incident description*, Paragraph 0040].

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beavers in further view of Frederick M. Avolio (*Best Practices in Network Security*, hereafter Avolio).

Regarding claim 3, Beavers states that *the threshold value can be a level of severity* [Paragraph 0013] and that severity is defined *on a scale of 1-5 (1 being the highest threat)* [Paragraph 0036]. Beavers does not explicitly disclose that the threshold value is inversely proportional to the node value.

However, Avolio teaches [Avolio: Page 2 Column 3] that the severity of a threat is based upon the value of the object (e.g., a node) being secured (i.e., such that the higher the value of an object, the lower the threshold value is set or *setting the threshold value inversely proportional to the node value*).

Beavers and Avolio are analogous subject matter in the same field of endeavor as both cover network security systems. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the threshold-severity relation taught by Beavers with the severity-value relation taught by Avolio because doing so allows for a basis by which to set the severity, and hence the threshold, level for object [Avolio: Page 2 Column 3].

Regarding claim 4, Beavers-Avolio teaches that the threshold value is inversely proportional to the service value [Avolio: Page 2 Columns 2-3, as the "object" can be a service].

Response to Arguments

9. Applicant's arguments filed 9 January 2008 have been fully considered, but not found persuasive.

10. Regarding independent claim 1, applicant argues the applied reference does not teach the claim limitations as recited. Namely, applicant argues that Beavers does not

teach *an authorization enforcement facility operable to perform a risk-aware analysis of [a] connection to determine the threat level associated with the connection based at least in part on [a] static policy data attribute.*

In response to the above-mentioned arguments, applicant's interpretation of applied prior art is noted. However, as examiner notes above, Beavers does teach an authorization enforcement facility (AEF) [*alert processing system,* claim 12, figure 5 (63)] in communication with the static policy data store [*Rule Engine*, Figure 5 (27)] and the dynamic policy data store [*Decision Tables*, Figure 5 (31)] and operable to perform a risk-aware analysis [*matching* and *declaring an incident*, claim 1] of the connection [via *firewall* of Paragraphs 0002-0003 and connection-monitoring *device experts* of Paragraphs 0104-0114] to determine the threat level [*alert indication* containing a *level of severity*, Paragraph 0013] associated with the connection based at least in part on the static policy data attribute [*static enterprise data... such as lists of IP addresses that are associated with known attackers,* Paragraph 0077].

11. Regarding independent claim 13, applicant argues the applied reference does not teach the claim limitations as recited. Namely, applicant argues that Beavers does not teach *determining a threat level associated with [a] connection based at least in part on [a] static policy data attribute.*

This argument is substantially the same as for claim 1.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IMAD HUSSAIN whose telephone number is (571) 270-3628. The examiner can normally be reached on Monday through Friday from 0730 to 1430.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/IH/
Imad Hussain
Examiner

ABDULLAHI SALAD
PRIMARY EXAMINER